

Web · Images · Groups · Directory · News ·

Searched the web for **xtr gf**.

Results 1 - 10 of about 4,030. Search took 0.17 seconds.

Tip: In most browsers you can just hit the return key instead of clicking on the search button.

Need to mention conjugates (sum of all roots in **GF(pn)**)

... The Galois Field used by **XTR**, **GF(p 6)***, has order $p^6 - 1$. This format is taken advantage of when choosing the subgroup for **XTR**. ...

www.cs.rit.edu/~wen2559/XTR_2.html - 44k - Cached - Similar pages

The XTR Cryptosystem

... **XTR** uses Galois Fields, denoted **GF(p n)**. A Galois Field is a finite extension field of characteristic p and extension of degree n . Galois Fields are finite ...

www.cs.rit.edu/~wen2559/XTR.html - 20k - Cached - Similar pages

[More results from www.cs.rit.edu]

[PDF] Improving XTR

File Format: PDF/Adobe Acrobat - [View as HTML](#)

MIT Laboratory for Computer Science, March 2003 335 Improving **XTR** David Woodruff, Marten ... protocol, Alice and Bob work over some finite field **GF** ' p^6 , Alice ...

www.csail.mit.edu/research/abstracts/abstracts03/theory/65woodruff.pdf - Similar pages

[PPT] The XTR Public Key System

File Format: Microsoft Powerpoint 97 - [View as HTML](#)

... RSA, ECC, **XTR**. Element representation of **GF(p2)**. Let $p \equiv 2 \pmod{3}$, then and p form an ONB for **GF(p2)** \times **GF(p2)**, $x = x_1 + x_2 p = x_1 + x_2 2$. Trace. ...

algo.csie.nctu.edu.tw/upload/slide/The%20XTR%20Public%20Key%20System.ppt - Similar pages

gf

... **gf**: FRAME, rocky mountain element to. SHOCK, sid. BOT. BRACKET, race face. CRANKS, race face. CHAINRINGS, race face. PEDALS, time atac. FRONT DER, **xtr**. CHAIN, **xtr**. REAR DER, **xtr** ...

www.mtbreview.com/dream/bikes/8950.html - 16k - Cached - Similar pages

[PDF] The XTR public key system

File Format: PDF/Adobe Acrobat

... representation in cryptographic protocols is provably as secure as using the traditional representation in **GF(p 6)** • either **XTR** is secure (because **GF(p 6)** ...

home.hetnet.nl/~ecstr/msri_xtr.pdf - Similar pages

SpringerLink - Chapter

... **XTR** Extended to **GF(p)** Seongan Lim A1 , Seungjoo Kim A1 , Ikkwon Yie

A2 , Jaemoon Kim A2 , Hongsub Lee A1. A1 KISA (Korea Information ...

link.springer.de/link/service/series/0558/bibs/2259/22590301.htm - 18k - Nov 20, 2003 - Cached - Similar pages

[PDF] Presentaties met PDFScreen

File Format: PDF/Adobe Acrobat - [View as HTML](#)

... 1 and where $p \equiv 2 \pmod{3}$. Claim: **XTR** achieves the communication advantages and computational costs of **GF(p 2)** but has the security of **GF(p 6)**. This is ...

www.stork.eu.org/slides/15_stork-henk.pdf - Similar pages

XTR

... http://www.comp.mq.edu.au/~igor/Publ.htm; Seongan Lim, Seungjoo Kim, Ikkwon Yie, Jaemoon Kim, Hongsub Lee: "XTR Extended to GF(p^{6m})", Selected Areas in ...
www.kisa.or.kr/technology/sub1/XTR.htm - 14k - Cached - Similar pages

[PPT] www.cacr.math.uwaterloo.ca/conferences/2000/ecc2000/lenstra.ppt

File Format: Microsoft Powerpoint 97 - [View as HTML](#)

... as secure as traditional versions over GF(p6). either XTR is secure (because GF(p6) is secure). ... Either XTR is secure or GF(p6) is not as secure as believed. ...

[Similar pages](#)

Gooooooooogle ►

Result Page: [1](#) [2](#) [3](#) [4](#) [5](#) [6](#) [7](#) [8](#) [9](#) [10](#) [Next](#)

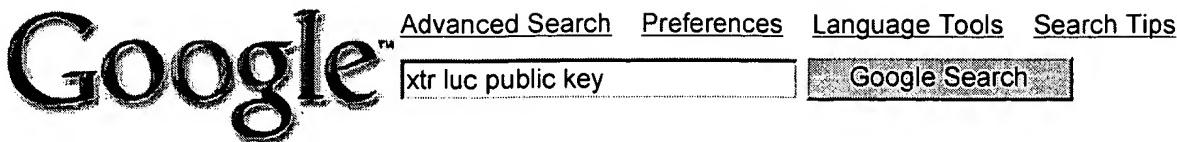
Dissatisfied with your search results? [Help us improve.](#)

Get the [Google Toolbar](#):



[Google Home](#) - Advertise with Us - Business Solutions - Services & Tools - Jobs, Press, & Help

©2003 Google



[Public Key - Messaging Security Toolkits for Developers](#)

www.phaos.com Messaging Security From the E-Security Leader - CLICK Now!

Sponsored Link

[PDF] [The XTR public key system](#)

File Format: PDF/Adobe Acrobat

The **XTR public key** system Arjen K. Lenstra Citibank, New York ... to represent subgroup elements (like **LUC**, but better) • The security of **XTR** is based on ...

home.hetnet.nl/~ecstr/msri_xtr.pdf - [Similar pages](#)

[Thoughts on cipher selection from Joseph Ashwood on 2000-12-12 \(...](#)

... **Public key** encryption. ... Of course we need to support RSA-OAEP, but we should also support EC-EIGamal, **XTR**, NTRU, EIGamal, RPK, ACE, **LUC**-EIGamal, etc. ...

lists.w3.org/Archives/Public/xml-encryption/ 2000Dec/0010.html - 12k - [Cached](#) - [Similar pages](#)

[SSH : Support : Cryptography AZ : Algorithms : Public Key ...](#)

... with **XTR** ideas. So in a way **XTR** is a generic name for a class of **public key** algorithms, similarly to **LUC**. Perhaps surprisingly, the ...

www.ssh.fi/support/cryptography/ algorithms/asymmetric.html - 51k - [Cached](#) - [Similar pages](#)

[Public Key Cryptography: Concrete Systems](#)

... Novel usage of **XTR** in cryptographic protocols: A Practical ... and some Applications of Paillier's Probabilistic **Public-Key** System (Ivan ... **LUC** family; @McEliece ...

www.tcs.hut.fi/~helger/crypto/ link/public/concrete.html - 9k - Nov 20, 2003 - [Cached](#) - [Similar pages](#)

XTR

... A. Lenstra, E. Verheul, "The **XTR public key** system", Advances in ... nl/~ecstr/mathdetails.htm.
PJ Smith, MJJ Lennon, "LUC : A New **Public Key** System," Proceedings ...

www.kisa.or.kr/technology/sub1/XTR.htm - 14k - [Cached](#) - [Similar pages](#)

[ATableofPublic-KeyCryptosystems](#)

... pq. RSA; Rabin; Rabin-Williams; Dickson; **LUC**; PSS. ... EIGamalSig; DSA; KCDSA; **XTR**. [Key Distribution Scheme]. UP. ... New **Public Key** Cryptosystem Using Finite Non Abelian Groups. ...

www.kisa.or.kr/technology/sub1/menu.htm - 22k - [Cached](#) - [Similar pages](#)

[PDF] [An overview of the XTR public key system](#)

File Format: PDF/Adobe Acrobat - [View as HTML](#)

An overview of the **XTR public key** system Arjen K. Lenstra 1 , Eric R. Verheul 2 1
Citibank, NA, and ... **XTR** is not the first method to do so ... The **LUC** cryptosystem (cf ...

www.win.tue.nl/~klenstra/xtrsurvey.pdf - [Similar pages](#)

[PDF] [More Public Key Cryptography](#)

File Format: PDF/Adobe Acrobat - [View as HTML](#)

... 18, 2003 Advanced Cryptography - Week 10 32 **Public Key** Algorithms Integer Factorization Discrete Logarithm RSA GQ ESIGN Diffie-Hellman DSA, NR **XTR LUC** El-Gamal ...

www.isg.rhul.ac.uk/msc/teaching/opt8/week10.pdf - [Similar pages](#)

[\[PDF\] 10.3. GH-DSA](#)File Format: PDF/Adobe Acrobat - [View as HTML](#)

... P. Smith, "LUC public-key encryption," Dr. Dobb's Journal ... this family of the **public-key** cryptosystems is a ... and ER Verheul, The **XTR** public key systems, Advances ... calliope.uwaterloo.ca/~ggong/ECE710T4/lec12-ch10b.pdf - [Similar pages](#)

[MPKC 2003: Mathematics of Public-Key Cryptography](#)

... of the constructions of **public-key** cryptography--and ... Abstract: "Key compression; reducing randomness ... a mathematical interpretation of **LUC**, **XTR**, and conjectured ...

mpkc2003.mwisc.org/ - 24k - Nov 20, 2003 - [Cached](#) - [Similar pages](#)

Gooooooooogle ►

Result Page: [1](#) [2](#) [3](#) [4](#) [5](#) [6](#) [7](#) [8](#) [9](#) [10](#) [Next](#) Dissatisfied with your search results? [Help us improve.](#)Get the [Google Toolbar](#):[Google Home](#) - Advertise with Us - Business Solutions - Services & Tools - Jobs, Press, & Help

©2003 Google